2. Барановский, Н. Научно-практическая модель системы предупреждения преступности / Н. Барановский, Н. Шевчук // Юстыцыя Беларусі. – 2012. – № 7. – С. 37–41.

3. Белокопытов, В. В. Алкоголизм и преступность (часть 1) [Электронный ресурс] : [по состоянию на 10.06.2015 г.] / В. В. Белокопытов, В. М. Филиппенков // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2017.

4. Министерство внутренних дел Республики Беларусь [Электронный ресурс]. – Режим доступа: http://mvd.gov.by/. – Дата доступа: 10.01.2017.

УДК 341.4

О. И. Левшук
старший преподаватель кафедры
административной деятельности ОВД
факультета милиции УО «Академия
Министерства внутренних дел Республики Беларусь»,
кандидат юридических наук

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ: МЕЖДУНАРОДНЫЙ ОПЫТ

Внедрение цифровых технологий и глобализация компьютерных сетей вынуждают искать пути противодействия кибепреступности, ставшей общемировой угрозой современному обществу. Защита физических и юридических лиц при автоматизированной обработке данных от противоправных посягательств является одной из задач, стоящих перед правоохранительными органами. Согласно Конвенции о преступности в сфере компьютерной информации (ETS № 185), принятой 23 ноября 2001 г. в Будапеште, признается преступлением умышленно осуществленный с использованием технических средств перехват компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, а также умышленное создание помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных [1].

Мировое сообщество сегодня обеспокоено распространенностью преступлений, совершаемых в сфере компьютерной информации. Отдельные хакеры используют вирусную программу &#8220ransomware&#8221, которая запаковывает важные документы в закодированный архив и удаляет их оригиналы, делая таким образом невозможным доступ к ним до момента уплаты выкупа. Случаи таких вымогательств встречаются во всем мире очень часто. Объектом внимания киберпреступников становятся сведения о персональных данных пациентов медучреждений, о составе медицинских препаратов,

указанных в электронных медицинских картах. Имели место факты, когда преступники меняли данные производителей (торговой организации) лекарственных препаратов, вписанных в медицинские карты пациентов. Так, руководство регионального медицинского центра «Titus» в Маунт-Плезант было вынуждено перечислить в качестве выкупа деньги хакерам, заблокировавшим в январе 2016 г. доступ медперсонала к электронным медицинским картам пациентов. Жертвой хакерской атаки стала индийская фармацевтическая компания, выплатившая немалую сумму денег за получение доступа к заблокированным данным [2, с. 12].

По данным ФБР в 2015 году, в США киберпреступникам было выплачено в качестве выкупа 25 млн долларов США, а за три месяца 2016 г. – 209 млн долларов США. По числу случаев применения вредоносного программного обеспечения лидируют Япония, Австралия, Индия, Турция.

Одним из резонансных случаев явилась кибератака на германский сталелитейный комбинат. Отправленные фишинговые сообщения по электронной почте позволили получить доступ к компьютерной системе компании. Киберпрограмма отключила компоненты централизованного контроля и технологического оборудования, вследствие чего прекратилось электроснабжение и была выведена из строя система управления доменной печью. Компания понесла весьма крупный ущерб от действий злоумышленников [3, с. 19–20].

Полицейские структуры также подвергаются кибератакам, в результате которых персональная информация о сотрудниках полиции и их семьях, конфиденциальные сведения о спецоперациях правоохранительных органов похищались из цифровых файлов и предавались огласке. После взлома компьютерной системы также изменялось либо вовсе удалялось досье преступников.

Возможности современных технологий, Интернета и социальных сетей могут применяться в целях планирования терактов и их реализации, дестабилизации экономического состояния государства либо отдельных объектов инфраструктуры, проникновения в информационные системы правоохранительных и иных государственных органов для похищения, распространения информации или блокирования доступа к информационной базе с целью вымогательства денег [4, с. 8].

Распространенность таких угроз сегодня во всем мире обусловливает поиск новых подходов по обеспечению информационной безопасности и разработку мер по противодействию киберпреступности. В частности, одним из средств защиты является установление современных версий программных продуктов, к которым относятся программы, использующие идентификацию подписи, поведенческий анализ; антивирусные программы; средства сетевой защиты; датчики проникновения; защитные программные продукты. Одновременно и инструктирование сотрудников организаций по безопасному использованию сети Интернет является условием обеспечения сохранности электронной информации [2, с. 15].

Для противодействия кибератакам создан Кибернетический центр правоохранительных органов (КЦПО) – онлай-ресурс, предназначенный для руководителей правоохранительных органов всех уровней (SLTT LEAs), экспертов по киберпреступности и криминалистов, специалистов быстрого реагирования и прокуроров. К числу задач центра относятся: демистифицирование сферы обеспечения кибербезопасности с учетом технических возможностей и обмена информации; оказание помощи в расследовании киберпреступлений и преступлений с использованием киберсредств; обеспечение сбора, сортировки и анализа цифровых улик. Цель создания данного центра – обеспечить правоохранительным органам быстрый и простой доступ к лучшим ресурсам, документам и видео, подготовленным в интересах руководителей правоохранительных органов [4, с. 12].

С учетом того, что основной причиной кибератак является недостаточность мер защиты информационных систем, намечено три основных направления в обеспечении безопасности инфраструктурных объектов: интегрирование различных систем обеспечения безопасности на объединенной односистемной платформе; широкое использование термовидеокамер и пакетов аналитических программ; внедрение биометрических пакетов в системе физической безопасности [3, с. 25].

Таким образом, преступления в сфере информационных технологий (киберпреступность), имея транснациональный характер, представляют реальную угрозу для организаций государственной и частной форм собственности, их нормальному функционированию. Такие противоправные деяния могут совершаться не только в отношении персональных компьютеров, но и мобильных телефонов, планшетов. А поэтому мировое сообщество должно быть бдительным и принимать всевозможные меры по недопущению взлома паролей, хищения либо искажения информации, имеющейся в электронных устройствах, вмешательства в работу различных систем посредством сети Интернет, а также совершения иных противоправных действий.

Список основных источников

1. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [Электронный ресурс]. – Режим доступа: tttp://www.alpp.ru/law pravosudie/46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii-185rus-angl.html. – Дата доступа: 10.01.2017.

2. Компьютерное вымогательство: необходимость усиления информационной безопасности / пер. С. Велев // Борьба с преступностью за рубежом: по материалам иностр. печ. – 2016. – № 7. – С. 11–15.

3. Угроза кибератак на жизненно важную инфраструктуру США / пер. С. Велев // Борьба с преступностью за рубежом: по материалам иностр. печ. – 2016. – № 10. – С. 19–27.

4. Кибератаки: современная террористическая угроза / пер. С. Берец // Борьба с преступностью за рубежом: по материалам иностр. печ. – 2016. – № 9. – С. 7–13.